**REPORT**

**Yêu cầu:** Khai thác máy tính bằng Buffer Overflow ( tràn bộ nhớ đệm ) để có thể truy cập vào root để chiếm quyền điều hành máy. Đồng thời hãy bảo vệ máy khỏi Buffer Overflow.

**Kịch bản:** Sử dụng máy ảo Kali Linux ( 32 bit ). **i686** là 32bit. Thực hiện các commands và scripts để thực hiện quá trình Buffer Overflow.

A screenshot of a computer

AI-generated content may be incorrect.

**Công cụ / mô hình:** Sử dụng Vmware Workstation Pro version 17.8 để thực hiện, và được cung cấp scripts để tấn công (stack.c và exploit.c). ( [Buffer-Overflow Vulnerability Lab](https://seedsecuritylabs.org/Labs_16.04/Software/Buffer_Overflow/) ).

**Setup:**

A screenshot of a computer

AI-generated content may be incorrect. A screenshot of a computer

AI-generated content may be incorrect.

**Steps:**

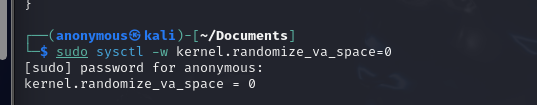
**Tấn công Buffer Overflow**

Truy cập đường link [Buffer-Overflow Vulnerability Lab](https://seedsecuritylabs.org/Labs_16.04/Software/Buffer_Overflow/) để lấy scripts là stack.c và exploit.c sau đó lưu vô tập tin Documents.

A screenshot of a computer

AI-generated content may be incorrect.

Tiếp theo ta phải tắt chức năng random ( **ASLR** ) địa chỉ thanh ghi bằng lệnh ( $sudo sysctl -w kernel.randomize\_va\_space=0 ). Khi kernel.randomize\_va\_space=0 tức là đã tắt chức năng random rồi.



Tạo file debug stack từ stack.c

A screen shot of a computer

AI-generated content may be incorrect.

Tạo badfile



Tiếp đến hãy debug file stack\_dbg để tìm địa chỉ thanh ghi ebp và địa chỉ buffer để tính khoảng cách từ buffer đến ebp để ghi đè lên return address.

A screenshot of a computer screen

AI-generated content may be incorrect.

Ta ra được địa chỉ của thanh ghi ebp và buffer

A screenshot of a computer code

AI-generated content may be incorrect.

Sau đó lấy địa chỉ thanh ghi ebp trừ đi buffer rồi + 4 để trả về return address

A screenshot of a computer

AI-generated content may be incorrect.

A screen shot of a computer screen

AI-generated content may be incorrect.

Tiếp theo sẽ edit trên scripts exploit.c viết them dòng code:

\*((long \*) (buffer + 36)) = 0xbfffed28 + 0x80 //offset chọn ngẫu nhiên tránh trường hợp “\0”.

memcpy(buffer + sizeof(buffer) – sizeof(shellcode), shellcode, sizeof(shellcode));

A screenshot of a computer screen

AI-generated content may be incorrect.

( $sudo ln -sf /bin/zsh/bin/sh ). Sau khi chạy lệnh trên, mọi lệnh hoặc script gọi /bin/sh sẽ thực sự chạy **Zsh** thay vì shell mặc định.

Biên dịch chương trình với stack có thể thực thi và không có bảo vệ → Dễ dàng kiểm tra, khai thác buffer overflow hoặc chạy shellcode trên stack ( $gcc -DBUF\_SIZE=24 -o stack -z execstack -fno-stack-protector stack.c ).

A screen shot of a computer

AI-generated content may be incorrect.

Cấp phép quyền root cho và SET-UID quyền đọc ghi thực thi,… file stack.

A screenshot of a computer

AI-generated content may be incorrect.

Tạo file debug exploit từ explot.c

A screen shot of a computer

AI-generated content may be incorrect.

Thực thi truy cập **root shell**



**Bảo vệ khỏi Buffer Overflow**

Bật **ASLR** ( $sudo sysctl –w kernel.randomize\_va\_space=2 ). Khi randomize\_va\_space=2 thì ngẫu nhiên hóa toàn bộ không gian địa chỉ làm tang cường bảo mật.

A computer code with white text

AI-generated content may be incorrect.

Mở bảo vệ StackGuard để bảo vệ stack trong trình biên dịch giúp phát hiện buffer overflow khi không dùng cờ -fno-stack-protector vì biên dịch sẽ tắt StackGuard, ta chỉ nên biên dịch bình thường. Exp: ( $gcc -o stack stack.c )

Bật Non-Execute Stack Protection để không cho phép thực thi mã trên stack giúp bảo vệ khỏi shellcode injection . Exp: ( $gcc -o stack -fno-stack-protector -z noexecstack stack.c )

**Results:**

Truy cập root shell:



**Đánh giá:**

Tấn công **Buffer Overflow** xảy ra khi một chương trình ghi dữ liệu vượt quá kích thước của bộ đệm (buffer), dẫn đến ghi đè lên các vùng nhớ lân cận. Lỗ hổng này có thể bị khai thác để làm chương trình bị crash, thực thi mã độc hoặc thậm chí chiếm quyền điều khiển hệ thống.

Dẫn đến các hậu quả tấn công từ xa thực thi mã độc trên hệ thống mục tiêu, leo thang đặc quyền lợi dụng để chiếm quyền root/admin. Làm gián đoạn dịch vụ (DoS) gây crash ứng dụng hoặc hệ thống

Hãy bật ASLR, DEP, Stack Canaries để bật cơ chế bảo vệ bộ nhớ tránh Buffer Overflow.